Defense Trade Advisory Group

DDTC and DSS Oversight of Unclassified Technical Data

Plenary Session October 25, 2018

Agenda



- Working Group Members
- Tasking
- Issues/Topics
 - Problem identification
 - Illustrative examples
- Recommendations
- Questions and Discussion

Working Group Members



- Beran, Mary
 Georgia Tech Research Corp.
- Cinelli, Giovanna*
 Morgan, Lewis & Bockius LLP
- Cross, Sandra
 Huntington Ingalls Industries
- Fujiu, Melanie
 United Launch Alliance, LLC
- **Keefer, Cynthia** BAE Systems, Inc.
- Miller, Michael
 University of Central Florida

- Millsaps, Mary Purdue University
- Novis, Ari
 Pratt & Whitney Aircraft
- Reeves, Johanna*
 Reeves & Dola, LLP
- **Rill, Dale**Honeywell International Inc.
- Rowold, Gretta
 Langley Law Group
- Sears, Heather
 Global Compliance Counsel, LLC
- * Working Group Co-Chairs

Tasking



"The ITAR controls unclassified and classified technical data related to defense articles and defense services. In this context, the ITAR and the NISPOM (under the Defense Security Service (DSS) oversight) share jurisdiction related to classified [and unclassified] technical data related to defense articles and defense services. Given the potential for confusion, please address "any" potential issues related to the "potential" overlapping of jurisdiction and identify any matters that would benefit from potential future clarification within the ITAR that may alleviate potential confusion."

-- DTAG Tasking Letter, Jul. 25, 2018

Further Clarification on Tasking



- Determine whether a problem exists; what does industry see as the friction points of the inherent conflict between International Traffic in Arms Regulations (ITAR) and National Industry Security Program Operating Manual (NISPOM) responsibilities?
- If there is a problem, how can it be remedied through the ITAR, through interagency engagement, or potential fixes to the NISPOM?
- Confirm whether conclusions reached in the 2014
 DTAG tasking are still valid in light of ECR changes.

DTAG Approach to Tasking



What is the problem?

 Held discussions with industry representatives (working group then whole DTAG) to determine whether confusion exists regarding overlapping jurisdiction of DSS and DDTC.

Why is there a problem?

 Researched agency legal authority over exported unclassified information and recent expansion of DSS oversight.

How to solve the problem?

Identified possible solutions to address the problem.

What is the Problem?



- Confusion in industry over whether DSS has authority to review unclassified ITAR-controlled information & documents as part of their audits.
- DTAG addressed this issue in 2014 (January Plenary) as part of a tasking covering "Competing Controlled Unclassified Information and Critical Program Information (CUI/CPI)."
- Problems have persisted, but recent changes to legal landscape significantly impact how DSS views its role.

Legal Landscape – DDTC Authority



U.S. Department of State, Directorate of Defense Trade Controls

- Arms Export Control Act grants President the authority to control the export & import of defense articles & defense services (<u>classified & unclassified</u>).
- Jurisdiction over exports and temporary imports delegated to the Secretary of State -- Bureau of Industry and Security, Directorate of Defense Trade Controls (DDTC).
- DDTC regulations: International Traffic in Arms
 Regulations (22 C.F.R. § 120-130) (classified and unclassified defense articles/defense services).

DSS Historical Authority



Defense Security Service (DSS)

- Department of Defense (DOD) agency operating under authority and control of the Under Secretary of Defense for Intelligence (10 U.S.C. and DOD Directive 5143.01).
- Provides military services, defense agencies, federal agencies and cleared contractor facilities with security support services.
 - Serves as "interface" between government and cleared industry for cleared and counterintelligence activities. Supports the Department of Defense and cleared contractors in the classified and otherwise designated arenas.
- Administers and implements the defense portion of the National Industrial Security Program (NISP) pursuant to Executive Order 12829.

Controlled Unclassified Information



- Executive Order 13556 (Nov. 10, 2010) established program for managing information that requires safeguarding and dissemination controls.
- National Archives and Records Administration (NARA) –
 the Executive Agent (EA) charged with implementing the
 CUI Program and overseeing agency actions to ensure
 compliance with EO. https://www.archives.gov/cui
 - Approves categories and subcategories of CUI and associated markings.
 - Places CUI on the CUI registry; includes unclassified export controlled information and technical data (EAR & ITAR).
 - Regulations: 32 C.F.R. § 2002.

Purpose and Scope (32 C.F.R. § 2002.1)



- Address federal inconsistencies in marking and handling. Prior to CUI Program, agencies employed ad hoc agency-specific policies, procedures and markings to handle the information.
- NARA regulations apply to all executive branch agencies that designate or handle information that meets the standards for CUI (32 C.F.R. § 2002.1(f)).
- Does not apply directly to non-executive branch entities, but does apply indirectly to non-executive branch CUI recipients, through incorporation into agreements (gov't. contract).

DSS In Transition (Expanded Auth.)



- Agency once concentrated on schedule-driven NISPOM compliance now moving to an <u>intelligence-led, asset-focused, and threat-driven</u> <u>approach to industrial security oversight.</u>
- In response to higher foreign intelligence threat and increased attacks on cleared industry
- DSS moving forward in partnership with industry to design, develop, and pilot multidimensional approach to industrial security oversight.
- http://www.dss.mil/dit.html

DSS Authority Expanded to CUI



- Under Sec. Def. Memo, May 17, 2018
 ("Controlled Unclassified Information
 Implementation and Oversight for Defense
 Industrial Base" (DIB))
 - Designates DSS as DOD's lead in implementing procedures for oversight of DOD's CUI program.
 - Use Security and Counterintelligence resources and expertise to identify CUI with the potential to impact national security and oversee its protection across the DIB.

DSS Oversight Over CUI



- DSS Director is required to execute operational plan for oversight of CUI protection through collaboration with industry partners across the DIB.
- Within six months of date of memo (<u>Nov. 17</u>, <u>2018</u>), DSS Director shall issue an initial report addressing:
 - Identification of resource constraints;
 - Additional policy required to support CUI oversight authority;
 - Program improvement recommendations.

CUI: Roles and Responsibilities



Designate s CUI Categories

• Reviews/
approves
agency
policies to
implemen
t CUI
program

•Must safegu CUI at times

Agency

safeguard
CUI at all
times
• DOD
personnel
must
follow DOD
policy for

CUI

Industry

Must comply with CUI safeguard requirements identified in contract

Information Subject to ITAR & NARA



Technical Data

As defined in ITAR § 120.10

> CUI//EXPT CUI//EXPTR

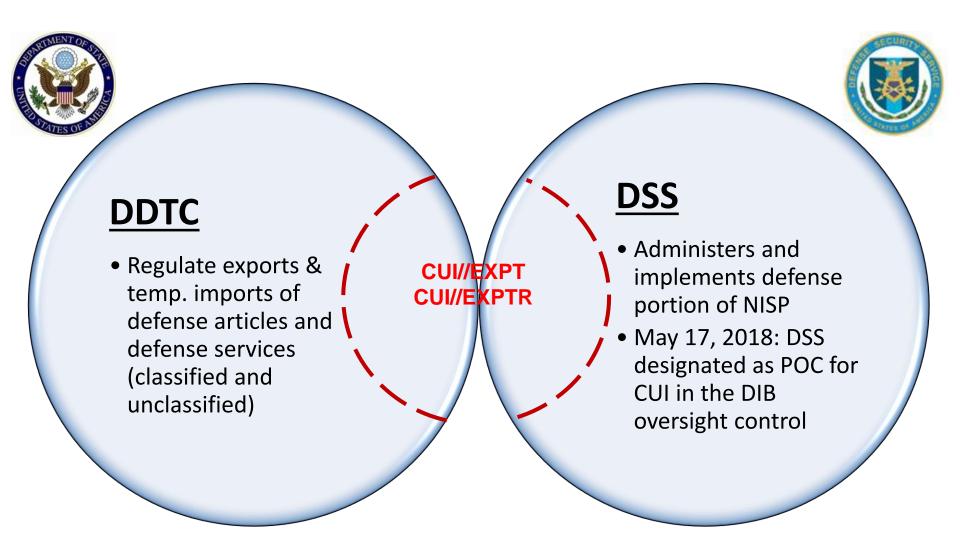
<u>CUI</u>

- As defined in 32
 C.F.R. § 2002.4(h)
- Possessed by or for an executive branch agency and;
- Subject to dissemination restrictions under FOIA 1-9

Note: not all CUI is export controlled, but all "technical data" is CUI if there is an underlying government contract identifying the CUI.

Regulatory Oversight of Unclassified Information







Conflicting Guidance on Perceived Authority

- DSS has stated that a license is not required for Classified items and defense services.
 - Ignores DSP-85, Classified TAAs....
- "USG-approved Classified visits (by Foreign Nationals) constitute an exemption to the licensing provisions of the ITAR."
 - NISPOM 10-507(a)
- Claim that NISPOM requires DSS to:
 - "Validate agreements or licenses"
 - Analogy: DSS asserting authority over Unclassified IRAD



Competing Disclosure Processes

- DSS requires disclosures to DSS first.
 - Does it preclude DDTC voluntary disclosure benefit?
 - ITAR § 127.12(b)(2)
- Cyber incident reporting requirement of 72 hours leaves little time to determine if ITAR is involved.
 - DFARS 252.204-7012(b)
- DSS including invalid "ITAR violation" findings in inspection reports.
- Need Coordinated Process.
 - Promotes cooperation with Regulators



Conflicting Jurisdiction Guidance

- DSS has stated that marking as Distribution B, C & D or FOUO are ITAR controlled (whether or not ITAR technical data are present).
- Conflate ITAR control with what can not be viewed by a non-U.S. person.
- ➤ Need Coordinated Guidance



Other

- DSS requests review of authorizations, proprietary data, and other protected information not related to classified items or CUI.
 - Unclassified TAAs
 - Family Education Rights and Privacy Act (FERPA) data
 - CUI treated as No Foreign (NOFORN)

Tasking & Recommendations



Tasking:

"... Given the potential for confusion, please address "any" potential issues related to the "potential" overlapping of jurisdiction and identify any matters that would benefit from potential future clarification within the ITAR that may alleviate potential confusion."

DTAG:

- DDTC should consider amending ITAR (§ 120.5 and § 127.5).
- DDTC should consider interagency engagement.

Suggested ITAR Revisions - § 120.5



DTAG recommends inserting the following language into 22 C.F.R. § 120.5(a) (Relation to regulations of other agencies; export of items subject to the EAR):

"The Defense Security Service (DSS) oversees compliance of the National Industrial Security Program and has been designated by the DOD Senior Agency Official for Implementing the oversight of that unclassified technical data, owned by or generated for the U.S. Department of Defense, which is Controlled Unclassified Information (CUI) (defined in 32 C.F.R. § 2002.4(h))."

Current ITAR References to DSS



- 22 C.F.R. § 127.5 (Authority of the Defense Security Service).
 - Only references "appropriate action to ensure compliance with DOD National Industrial Security Program Operating Manual (unless such requirements are in direct conflict with guidance provided by DDTC, in which case the latter guidance must be followed)."
- DSS charged with developing plan for implementing procedures for CUI oversight. ITAR
 § 127.5 should be updated to reflect this.

Suggested ITAR Revisions - § 127.5



- Once the DoD CUI protection plan is approved, § 127.5 should be expanded to recognize DSS oversight of CUI pursuant to the CUI Program, not just NISPOM compliance.
- Parenthetical qualifier will guidance from DDTC still supersede DSS guidance when in direct conflict?

Additional Recommendations Interagency Engagement



- Both agencies should address the jurisdictional overlap of CUI (also consider overlap with EAR – need to include Commerce in engagement).
- Coordinate processes (example: ITAR violations) and guidance (example: conflicting interpretations of licensing requirements).
- Due to the increased jurisdictional overlap, there needs to be increased coordination and education between the agencies.



Questions And Discussion

Definition of CUI (32 C.F.R. § 2002.4(h))

Controlled Unclassified Information (CUI) is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls...

CUI Categories and Subcategories



 Defined as "those types of information for which laws, regulations, or Government-wide policies require or permit agencies to exercise safeguarding or dissemination controls, and which the CUI EA [NARA] has approved and listed in the CUI Registry."

32 C.F.R. § 2002.4(k)

CUI Registry Grouping: Export Control



Categories:

- "Export Controlled" Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and the munitions list; license applications; and sensitive nuclear technology information.
- "Export Controlled Research" Related to the systematic investigation into and study of materials and sources in order to establish facts and reach new conclusions.